## Remarks

The following is in response to the Office Action dated March 22, 2004.

Per the above amendment, claims 7-10 and 17-20 have been cancelled.

Regarding claims 11, 14, 21, and 25, the Examiner alleges that the claimed methods and apparatuses are anticipated by or obvious from the system in Fig. 2B of Pinder et al (USP 6,105,134). It is respectfully submitted that the Examiner's allegation is without merit.

In Fig. 2B of Pinder et al, the demultiplexer 230 separates transport data stream (TDS) into encrypted multi-session key $E_{Kpr}$(MSK), encrypted control word (CW) $E_{MSK}$(CW) and encrypted service $E_{CW}$(SERVICE).

Firstly, it is assumed that the encrypted service $E_{CW}$(SERVICE), the encrypted control word (CW), and the encrypted multi-session key $E_{Kpr}$(MSK) in Pinder et al correspond to the encryption-resultant contents information, the encryption-resultant first-key base information, and the transmission-purpose key base information in the claimed invention, respectively.

The Examiner alleges that the memory 232 in Fig. 2B of Pinder et al generates an authentication value, and is the same as the steps of or the means for generating an authentication value in the claimed inventions.

According to Pinder et al, column 7, lines 3-22, the DHCT private key and associated DHCT public secure micro serial number are stored in the memory 232. Public secure micro serial number is provided so that demultiplexer 230 can select an encrypted multi-session key $E_{Kpr}$(MSK). Thus, the public secure micro serial number is used only to select the encrypted multi-session key $E_{Kpr}$(MSK).

According to the foregoing portion of Pinder et al, encrypted multi-session key $E_{Kpr}$(MSK) is decrypted in decryptor 234 using DHCT private key. The DHCT private key is used by the decryptor 234 only to decrypt the encrypted multi-session key $E_{Kpr}$(MSK).

As is clear from the above explanation, Pinder et al do not teach "the step of generating an authentication value" in claims 11 and 14, and "the means for generating an authentication value" in claims 21 and 25. Pinder et al neither disclose nor suggest the claimed-invention portion that an authentication value is generated from a decryption-side ID information peculiar to a decryption side and previously-fed ID information which has been generated by an encryption-resultant contents information provider side. Pinder et al do not disclose an authentication value. Therefore, Pinder et al do not teach the claimed-invention portion that the generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information.

Secondly, it is assumed that the decryptors 234, 236, and 238 in Pinder et al use a first function, a second function, and a third function, respectively.

In the claimed inventions, second-key base information is generated from the reproduced transmission-purpose key base information and the generated authentication value according to a first function.

In Pinder et al, since any authentication value does not exist, the decryptor 234 does not generate second-key base information from the reproduced transmission-purpose key base information (the encrypted multi-session key $E_{Kpr}$(MSK)) and the generated authentication value.

It is unreasonably assumed that the multi-session key MSK in Pinder et al is the same as the second-key base information in the claimed invention. In this case, it is thought that the unencrypted CW outputted from the decryptor 236 in Pinder et al is the same as the second key in the various variants of the claimed invention. The unencrypted

CW is used by the decryptor 238 to decrypt the encrypted service $E_{cw}$(SERVICE). Since the encrypted service $E_{cw}$(SERVICE) is assumed to be the encryption-resultant contents information in the claimed inventions, there occurs a contradiction to the claimed-invention portion that the reproduced encryption-resultant first-key base information (the encrypted control word (CW)) is decrypted into recovered first-key base information in response to the generated second-key signal.

Furthermore, there occurs a contradiction to the claimed-invention portion that the first-key signal is generated from the recovered first-key base information according to the third function. Also, there occurs a contradiction to the claimed-invention portion that the reproduced encryption-resultant contents information is decrypted in response to the generated first-key signal to recover original contents information.

As understood from the above explanation, the system in Fig. 2B of Pinder et al involves contradictions to or differences from the different variants of the claimed invention. As previously mentioned, Pinder et al neither disclose nor suggest the claimed-invention portion that an authentication value is generated from a decryption-side ID information peculiar to a decryption side and previously-fed ID information which has been generated by an encryption-resultant contents information provider side.

Therefore, it is respectfully submitted that claims 11, 14, 21, and 25 are patentable over Pinder et al.

It appears that the Examiner thinks the DHCT private key fed from the memory 232 to the decryptor 234 in Pinder et al to be the same as the authentication value in the claimed invention. The DHCT private key is merely stored in the memory 232, and is not generated by the memory 232 in response to any other information.

On the other hand, in the claimed invention, an authentication value is generated from decryption-side ID information peculiar to a decryption side and previously-fed ID information which has been generated by an encryption-resultant contents information provider side. Therefore, Pinder et al fail to teach the generation of an authentication value from other information (decryption-side ID information peculiar to a decryption side and previously-fed ID information which has been generated by an encryption-resultant contents information provider side).

The Examiner's view seems to be as follows. The decryptor 234 in Pinder et al is equivalent to the claimed-invention portion that second-key base information is generated from the reproduced transmission-purpose key base information and the generated authentication value according to a first function.

In Pinder et al, encrypted multi-session key $E_{Kpr}$(MSK) is decrypted in decryptor 234 using DHCT private key to provide multi-session key MSK. Thus, the decryptor 234 implements decryption rather than generation of second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function. Therefore, Pinder et al fail to teach the generation of second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function.

It is respectfully submitted that Widmer (USP 4,313,031) does not teach the foregoing differences of the claimed inventions from Pinder et al. Accordingly, claims 11-16, and 21-28 are believed to be patentable over Pinder et al and Widmer.

In view of the foregoing, the examiner is respectfully requested to reconsider the application and pass the same to issue at an early date.

Respectfully submitted,

Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
717 North Fayette Street
Alexandria, Virginia 22314
Phone: (703) 299-4090

Date: June 1 2004